Setup Guide

McAfee ePOAdvanced Suite Installer (eASI)

For use with the McAfee Endpoint Protection Suites

COPYRIGHT

Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator,
McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Before You Begin 4

Install your McAfee Endpoint Suite..... 6

Configure the McAfee ePO Server 8

Systems and the System Tree 9

Set Policies for endpoints 11

Create custom policies 17

Set tasks for endpoints 19

Create client tasks 21

Policy and task inheritance in the System Tree 22

Deploy the McAfee Agent 22

Use dashboards and queries 26

Summary 29

Appendix A: McAfee Device Control 30

Appendix B: List of included eASI best practice policies 33

Appendix C: References 37

Before You Begin…

Thank you for downloading the McAfee ePO Advanced Suite Installer. This guide is organized so you can evaluate McAfee Endpoint in a pilot environment consisting of a McAfee ePolicy Orchestrator® (McAfee ePO™) server and a number of client computers. The guide contains step-by-step instructions for many of the common configuration and policy options of the McAfee Endpoint Suites. It also brings you the benefit of pre-built best practice policies and configurations used by millions of ePolicy Orchestrator-managed systems, from SMB to largest enterprises.

Many links throughout the document lead to instructional videos or specific KB articles that provide additional information on relevant topics. Links to existing ePolicy Orchestrator 4.5 videos are generally applicable to version 4.6.

What's Included

Core components of McAfee Endpoint Protection suites included in this installation:

- McAfee ePolicy Orchestrator (McAfee ePO) 4.6.5
- McAfee Agent 4.6
- McAfee VirusScan® Enterprise 8.8 Patch 3
- McAfee Host Intrusion Prevention 8.0 Patch 2 for Desktops
- McAfee SiteAdvisor® Enterprise 3.5 Patch 1
- McAfee Web Filtering for Endpoint 3.5 Patch 1
- McAfee Device Control 9.2 Patch 1

Requirements

Following are the platform specifications supported by the installer.

Operating Systems	Windows 2003 Server SP2 Windows 2008 Server R2
.NET framework	.Net Framework v3.5
RAM	Minimum of 2GB
Free disk space	At least 10GB of free space on the target drive
Browsers	• Firefox 3.5 • Internet Explorer 7.0 • Firefox 3.6 • Internet Explorer 8.0
Database	• SQL Express 2005 (default) Additional databases supported: • Microsoft SQL Server 2005 (with Service Pack 3 or higher) • Microsoft SQL Server 2008: ➢ with Service Pack 1 ➢ with Service Pack 2 ➢ R2
8.3 Naming Convention	8.3 Naming Convention must be Enabled
Supported Languages	English, German, and Spanish

Virtualization Support

The installer supports use of several types of virtual infrastructure software including:

- Citrix XenServer 5.5 Update 2
- Microsoft Hyper-V Server 2008 R2
- VMware ESX 3.5 Update 4
- VMware ESX 4.0 Update 1

Notes

Active Directory

Although ePolicy Orchestrator does not require a Windows Active Directory Domain, AD is required for some of the more advanced management features, such as user-based policies, or using AD credentials for ePolicy Orchestrator user accounts.

McAfee Global Threat Intelligence (GTI)

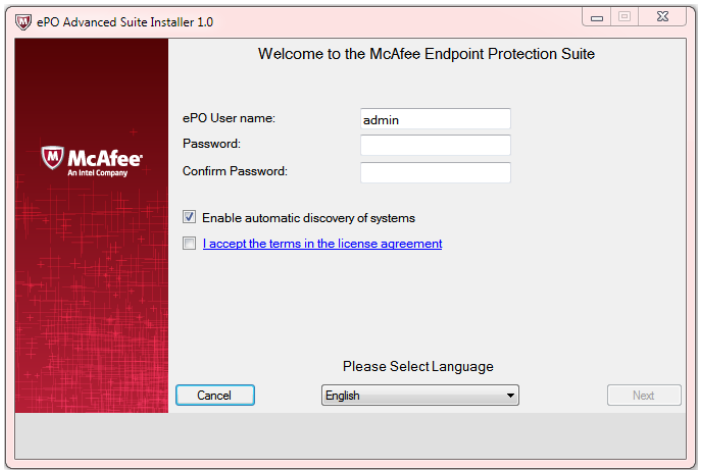
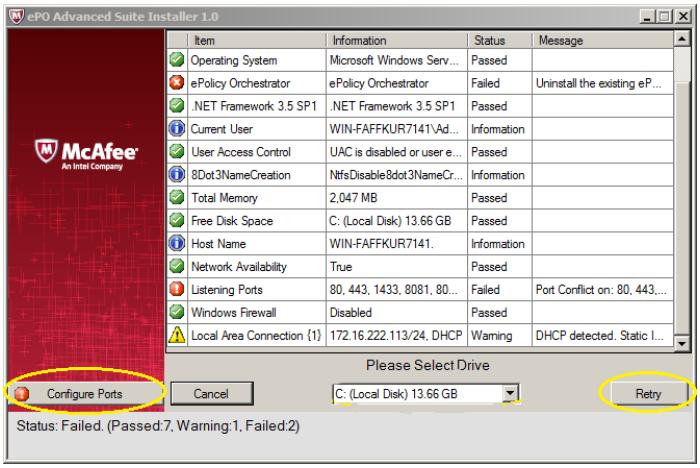
Throughout this document you will see references to McAfee's Global Threat Intelligence, or GTI. Today's changing threat landscape requires an advanced security solution that can proactively counter new threats. McAfee GTI hosts an extensive threat intelligence system in the cloud with visibility across all threat vectors — file, web, message, and network — and a view into the latest vulnerabilities across the IT industry. McAfee correlates real-world data collected from millions of sensors around the globe and delivers real-time, and often predictive, protection via its security products. Several products in the McAfee Endpoint Suites utilize GTI to protect McAfee customers every day. Policy examples in this guide cover how to take advantage of GTI technology.

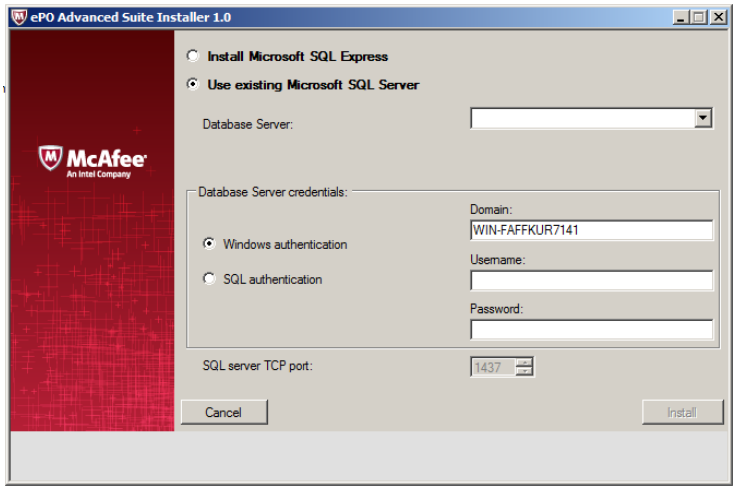
McAfee Application Control

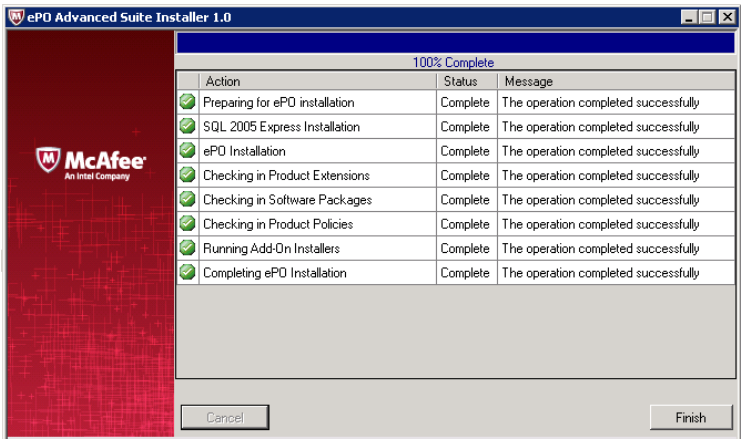
Looking to lock down and protect fixed-function devices, ATMs, cash registers, or SCADA systems? Consider McAfee Application Control, also managed by ePolicy Orchestrator.

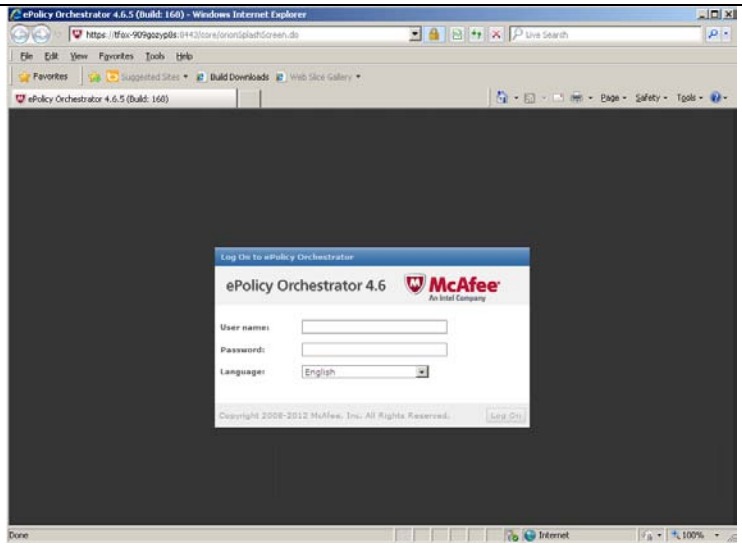
Install your McAfee Endpoint Suite

This section provides a walkthrough of the basic installation process. Make sure you have downloaded or copied the appropriate installer (eASIv1.0_EPS.zip or eASIv1.0_EPA.zip) and unzipped to a folder on your server.

Step #	Screenshot	Instructions
1		• Run **eASI.exe**. If UAC is enabled, right-click and **Run as Administrator**. • Enter a password to use for the ePolicy Orchestrator Admin account. Password must contain: ➢ At least 8 characters ➢ Upper and lowercase letters ➢ At least one numerical digit • By default, **Enable automatic discovery of systems** is checked, and will populate the ePolicy Orchestrator System Tree with machines found on the server's local subnet. • Click to accept the license agreement, and then click ***Next***.
2		• Verify the prerequisites. If any show the status of "Failed", check the Message column for details. • In case of port conflicts, click the **Configure Ports** button to assign different ports. • Remediate other issues, such as freeing up drive space or disabling the local firewalls, as needed, and then click the **Retry** button to rerun the prerequisite check.

3		Choose the database type:
		• **Install Microsoft SQL Express:** Select this option to install the default SQL Server Express 2005 software bundled with ePolicy Orchestrator.
		• **Use existing Microsoft SQL Server:** Select this option to connect to an existing database server on your network. Also supply the following information:
		  • Select a **Database Server** from the drop-down list. If not listed, enter it manually.
		  • Enter the desired authentication mode and valid **Database Server Credentials**.
		  • If you selected **SQL authentication**, the **SQL Server TCP port** is required. This number is auto-populated if the credentials are correct. If not, enter it manually.
		• Click **Install**.

4		Verify the installed components: • Verify the results on the resulting installation summary page. • Click **Finish** to complete. • If the installation is unsuccessful, please check the logs in the %temp% folder with the filename ***ePO.Advanced.Suite.Installer.xxxxx.log*** for any errors**.**

5		Upon completion, you are presented with the login page for McAfee ePO.

Configure the McAfee ePO Server

Log in to ePolicy Orchestrator

Log in with the User Name of **Admin** and the password that you designated during the installation.

On first login, you are presented with the Guided Configuration dashboard. Since the installer automated many of the basic configuration steps, including creation of a system tree plus client policies and tasks, we will bypass the Guided Configuration and dive straight in.

The ePolicy Orchestrator software repository

The McAfee ePO server is the central software repository for all McAfee product installations, updates, and other content. The modular design of ePolicy Orchestrator allows new products to be added as extensions. This includes new or updated versions of McAfee products, such as VirusScan Enterprise, and non-McAfee products from McAfee partners. Packages are components that are checked in to the master repository, and then deployed to client systems. ePolicy Orchestrator also allows for replication to distributed repositories at remote locations.

For McAfee ePO to keep your client systems up-to-date, a repository task that retrieves updates from a McAfee site (HTTP or FTP) was created to run daily at 1:00 am. The steps below show you how to modify the task so that it checks the McAfee update site every 12 hours.

Note that you can set any schedule you desire. There are generally two approaches — the standard approach similar to that described above, and a more advanced methodology to use if you are required to test signatures (DATs) on a subset of your systems prior to deployment to the remainder of your population. The standard approach is appropriate for most evaluations. Information on the advanced approach is detailed in the white paper Validating DAT and Other Content Files with McAfee ePolicy Orchestrator located on the McAfee Customer Portal.

Proxy configuration

NOTE: If you use a proxy server in your network environment, you will need to specify the configuration in the ePolicy Orchestrator Server Settings, so it can retrieve client updates and other content. If no proxy settings are required, skip to the following task, entitled Edit the repository pull task.

Configuring proxy settings

1 Click **Menu** | **Configuration** | **Server Settings**, select **Proxy Settings** from the Setting Categories, and then click **Edit**.
2 Select **Configure the proxy settings manually**, provide the specific configuration information your proxy server uses for each set of options, then click **Save**.

Editing the repository pull task

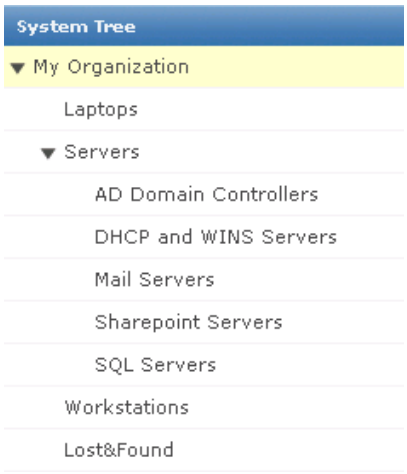
Follow the directions below to edit the default pull task so that ePolicy Orchestrator checks for updates every 12 hours. This is an example. You can set the schedule as required.

1 Click **Menu** | **Automation** | **Server Tasks**.
2 In the list, find the task named **Update Master Repository** and, under the **Actions** column, click **Edit** to open the Server Task Builder.
3 On the Description page, make sure **Schedule status** is set to **Enabled**, then click **Next**.
4 Select **Move existing packages to Previous branch**, then click **Next**.
NOTE: Checking this option allows ePolicy Orchestrator to maintain more than one set of signature files. When the task runs next, the current updates are moved to a directory on the server called Previous. This allows you to roll back updates if necessary.
5 On the Schedule page, choose when you want ePolicy Orchestrator to check the McAfee site for updates.
• Schedule the task to run **Hourly**, with **No End Date**.
• Set **Schedule** to every **12** hours.
6 Click **Next**.
7 On the Summary page, click **Save**. The console returns to the Server Tasks page.

Systems and the System Tree

The ePolicy Orchestrator System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions. These units are called groups, which are created and administered by Global Administrators or users with the appropriate permissions, and can include both systems and other groups.

As shown in the graphic below, the installer created a sample system tree during setup. Three groups were created under the default My Organization group; **Laptops**, **Servers**, and **Workstations**. Note that the Servers group also has several subgroups for different server types based on function or role.



Adding systems to your System Tree groups

If you chose Automatic Discovery of systems during the installation, use the following steps to organize your test systems in the System Tree. If you did not select Automatic Discovery, skip to the following task, entitled Adding systems manually.

Adding systems with Automatic Discovery

1 Click the **System Tree** button on the favorites bar.
2 Click on the **My Organization** group on the left. The systems are displayed on the right.
3 If there are any systems discovered that you do not want to be included in your testing, you can remove them from the tree. Place a check in the box next to all the systems you want to remove (you can use Shift+Click to select more than one), click **Actions | Directory Management | Delete**, and then click **OK**. You do NOT need to check the box for **Remove Agent on Next Agent-to-Server Communication**.
4 Drag and drop the remaining systems to their appropriate groups. You can drag multiple systems by placing a check mark by each first. A dialog box will appear asking "Are you sure you want to move the system(s)?". Click **OK**. You can check the box if you do not wish to see this dialog in the future.

Adding systems manually

1 In the **System Tree**, highlight the **Workstations** group and click **System Tree Actions | New Systems**.
2 For **How to Add Systems**, select **Add systems to the current group, but do not push agents**.
3 For **Target Systems**, type the NetBIOS name for each system in the text box, separated by commas, spaces, or line breaks. You can also click **Browse** to select systems.
4 Verify that **System Tree sorting** is disabled.

5 Click **OK**.
6 As needed, repeat these steps to add any servers to your Laptops or Servers group or its subgroups.

There are several methods of organizing and populating the System Tree:

- Manually structure your System Tree by creating your own groups and adding individual systems.
- Synchronize with Active Directory or NT domain as a source for systems. In the case of using Active Directory, synchronization mirrors AD and automatically provides System Tree structure.
- Create your own groups and sort based on IP ranges or subnets. This is called criteria-based sorting.
- Import a text file of groups and systems.

Quick Tip: If you wish to test system & group creation through Active Directory, detailed steps are provided in the McAfee Quick Tips video Active Directory Synchronization in ePO.

Set policies for endpoints

Policies are used to set the configuration for the various McAfee Endpoint products, such as VirusScan Enterprise, Host IPS, and many other products. Many pre-built best practice policies have been included as part the installer. They differ somewhat from the default policies in that some are designed for optimization and others to ensure endpoint clients function together in the most efficient manner. Note that these policies are not yet in effect. Within this guide we will discuss and apply several of these policies.

In a production environment, one would normally create and assign such policies in the System Tree before software is ever deployed. As such, the same approach will be used in your test deployment and evaluation.

The McAfee Agent policies

The McAfee Agent is the client-side component providing secure communication with ePolicy Orchestrator. It downloads and enforces policies, and handles client tasks such as deployment and updating for McAfee and McAfee-compatible, third-party products found at our Security Innovation Alliance.

Assigning a McAfee Agent policy globally

The following policy allows for remote viewing of the McAfee Agent log via browser and increases the Agent to Server Connection Interval (ASCI) from the default of 60 minutes to 120 minutes.

1 Click the **System Tree** button on the favorites bar.
2 Highlight **My Organization**.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **McAfee Agent**.
• On the line that lists **General**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI – General**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.

One reason to modify the Agent to Server Connection Interval on a group of systems might be to lessen the impact on already taxed WAN connections to remote sites, or simply because you are managing several thousand systems. See more information on the McAfee Agent in the Quick Tips video Controlling Agent Communication.

NOTE: To view the Agent Log on a remote system, type the following your web-browser: http://<computer_name_or_IP_address>:8081 where 8081 is the default port for the Agent Wake Up call. If you changed this port number during ePolicy Orchestrator installation, then use the port you specified. This can be very useful when you need to view the log for a system to which you do not have physical access; for instance, the system is on the other side of the country. You will be able to take advantage of this feature after we have deployed the Agent.

VirusScan Enterprise policies

Assigning a VirusScan policy to a group

Having assigned policies globally, the following applies policies to a specific group. Do you have one group of systems that has a higher probability of being exposed to malware than others? You are likely thinking of your laptop community and the common concerns around issues like non-standard images, use of unsecured wireless networks, or who is using the laptop and where they are surfing when off the corporate network. Setting GTI File reputation to High is used for systems or areas that have a greater susceptibility to being attacked.

Follow these steps to set GTI File Reputation to **High** for the **Laptops** group.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **Laptops** group.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **VirusScan Enterprise 8.8.0**.
• On the line that lists **On-Access General Policies**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI - Enable GTI for On-Access (High)**.
• Click **Save**.
For additional information on this feature, see the FAQs for Global Threat Intelligence File Reputation.

Assigning best practice VirusScan policies to the SQL Servers group

The installer includes many best practice server policies used by customers where the standard anti-virus (AV) defaults are not applicable. For instance, it is common practice to create AV exclusions on database servers, Microsoft Exchange servers, Domain Controllers, and so on. An extensive list of common exclusions can be found here: VirusScan Enterprise exclusions (Master Article). Details on available syntax are found in the VirusScan Enterprise 8.8 Product Guide.

Note also that McAfee VirusScan has the unique ability to vary scan settings based on the process in play at any given time. In the example below, *Sqlserver.exe* and *Sqlwriter.exe* are considered “low-risk” processes for spreading malware (unlike Explorer.exe, for example). Hence the policies are configured such that *scan on read* and *scan on write* are not active for those two select low-risk processes. Real customers combine this approach with traditional file and directory exclusions to provide the best server performance possible while limiting the threat of malware infection at the file system level. As such, a set of Low Risk and Default policies are used in concert.

Follow these steps to assign the Default Processes Policy to the SQL Servers group.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **SQL Servers** group.
3 Click the **Assigned Policies** tab.
4 From the **Product** drop-down menu, select **VirusScan Enterprise 8.8.0**.
5 On the line that lists **On-Access Default Processes Policies**, click **Edit Assignment**.
6 For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
7 From the **Assigned Policy** drop-down menu, select **EASI – Default: MS SQL Servers**.
8 Click **Save**.

Follow these steps to assign the Low-Risk Processes Policy to the SQL Servers group.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **SQL Servers** group.
3 Click the **Assigned Policies** tab.
4 From the **Product** drop-down menu, select **VirusScan Enterprise 8.8.0**.
5 On the line that lists **On-Access Low-Risk Processes Policies**, click **Edit Assignment**.
6 For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
7 From the **Assigned Policy** drop-down menu, select **EASI – Low: MS SQL Servers**.
8 Click **Save**.

Here's another way of looking at the type of policies you just assigned.

- A Low Risk Processes policy has process exclusions specific to the system type to which it is being deployed. In other words, VirusScan might scan little or nothing for a select group of low-risk processes as configured, such as sqlserver.exe and sqlwriter.exe.
- A Default Processes policy has common file & directory exclusions specific to the system type to which it is being deployed. File reads and writes by any process not classified as Low-Risk will trigger normal file scanning, except on the database and other key files and directories, i.e., your standard AV exclusions.

Quick Tip: Standard desktops and file servers might use a Default-only policy, as process exclusions are not typically required. You can get additional information on Risk-Based Scanning from the McAfee Knowledgebase articles KB55139 and KB66036, and the McAfee Quick Tips video What is Risk Based Scanning?.

Host IPS policies

Please note that McAfee Host IPS has two main components: kernel-level IPS protection and a firewall. The McAfee EPS suite contains the firewall only, while the EPA suite contains both components. If you are evaluating the EPS suite, skip to the section entitled **Host IPS Firewall**.

The main function of McAfee Host IPS is to protect systems against known and unknown attacks. This is often achieved without an update to the software, by use of patented buffer overflow and other behavioral protection. It has the additional benefit reducing the urgency and frequency of patching by protecting vulnerabilities from exploit even before a patch has been applied. Consider the time spent on patching within your organization. By deploying Host IPS, many of those vulnerabilities would be protected from exploit, allowing you to patch on a more reasonable schedule. For example, McAfee Host IPS protected against 60% of all exploits against Microsoft vulnerabilities, and nearly 75% of all exploits against Adobe vulnerabilities, disclosed between 2006 and 2011. Also consider the Host IPS ability to protect systems against exploit on those occasions when a new vulnerability exists but the corresponding patch is not yet available.

Perhaps you have shied away from Host IPS, feeling that it would be a complex or lengthy process to deploy, or had concern about blocking legitimate processes. By following a logical, systematic approach, you can quickly realize the benefits of deploying Host IPS in your environment. While the policies applied here are sufficient for initial testing, prior to full production deployment you are strongly encouraged to read over the deployment methodology discussed in detail in the Host IPS 8.0 Installation Guide, pp. 11-26.

Kernel Level Host IPS

For the initial stages of this evaluation, you will assign a policy that instructs Host IPS to block High severity events. This is essential if you plan to use attack tools to test the product's effectiveness. This is combined with logging of Medium and Low severity events. Apart from only logging events, this is often a typical first implementation in live environments.

Enabling Host IPS

Follow these steps to assign a policy that enables Host IPS on your client systems.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **Workstations** group.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **Host Intrusion Prevention 8.0: IPS**.
• On the line that lists **IPS Options**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI – HIPS Enabled**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.
4 Repeat the above steps for your **Laptops** group.

Setting Protection Level

Follow these steps to assign a policy that blocks High severity events, and logs any of Medium and Low severity. Logging provides detailed advanced knowledge of which signatures may require exclusions prior to enforcing block on Medium events, thus guiding accurate policy tuning. One can elevate select Low severity signatures to Medium later if desired, instead of maintaining all Lows active.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **Workstations** group.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **Host Intrusion Prevention 8.0: IPS**.
• On the line that lists **IPS Protection**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI - Block High Events**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.
4 Repeat the above steps for your **Laptops** group.

Assigning IPS Rules

As virtual systems are often used for evaluations, assigning this policy facilitates testing by changing VMWare protection signatures to a severity of Low. The McAfee Default policy maintains these signatures at their normal severity levels and should be considered before staging in a live environment.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **Workstations** group.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **Host Intrusion Prevention 8.0: IPS**.

• On the line that lists **IPS Rules**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI - VMware exception policy**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.
4 Repeat the above steps for your **Laptops** group.

Host IPS Firewall

The firewall is stateful and offers location awareness and other advanced features, including IP reputation filtering, part of McAfee's Global Threat Intelligence (GTI). The Host IPS Firewall uses GTI to protect endpoints from botnets, distributed denial-of-service (DDoS) attacks, command and control activity, advanced persistent threats, and risky web connections.

McAfee collects data from billions of IP addresses and network ports, and calculates a reputation score based on network traffic, including port, destination, protocol, and inbound and outbound connection requests. The score reflects the likelihood that a network connection poses a threat, such as a connection associated with botnet control.

Coupling a single firewall rule with a GTI-only policy lets you immediately receive the benefit of cloud intelligence on known botnets and command and control centers. This is achieved with little effort, minimal overhead, and no interference with your existing host or network firewall rules.

Enabling the Firewall

Follow these steps to assign a policy that simply enables the firewall and sets the sensitivity level for GTI at Medium risk or higher. At this point, no firewall ruleset is active or assigned.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **Workstations** group.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **Host Intrusion Prevention 8.0: Firewall**.
• On the line that lists **Firewall Options**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI – Enable FW and GTI**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.
4 Repeat the above steps for your **Laptops** group.

Configuring the GTI–Only Ruleset

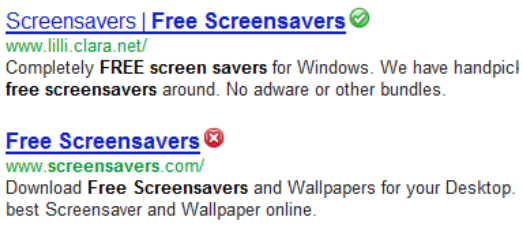
The steps below assign a policy that allows all traffic, but uses GTI to perform lookups of IP reputations and block connections to\from any posing a threat.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **Workstations** group.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **Host Intrusion Prevention 8.0: Firewall**.
• On the line that lists **Firewall Rules**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI – GTI Only**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.
4 Repeat the above steps for your **Laptops** group.

Answers to many common questions can be found in the FAQ for Host Intrusion Prevention 8.0.

SiteAdvisor Enterprise and Web Filtering for Endpoint policies

McAfee SiteAdvisor Enterprise leverages McAfee Global Threat Intelligence to provide reputation ratings for web sites using a color-coded system — primarily Red, Yellow, and Green, based on the risk associated with a given site (for example, “Red sites” hosting malware). Annotations are made in the browser, in search engine results (shown below), as well as links in IM and email programs such as Microsoft Outlook and Outlook Express.


Screensavers | Free Screensavers
www.lilli.clara.net/
Completely FREE screen savers for Windows. We have handpicl
free screensavers around. No adware or other bundles.
Free Screensavers
www.screensavers.com/
Download Free Screensavers and Wallpapers for your Desktop.
best Screensaver and Wallpaper online.

By combining Web Filtering for Endpoint with SiteAdvisor, administrators can also enforce policies regarding content categories, such as pornography, gambling, and other undesired sites. The two components are managed via the SiteAdvisor policies.

Administrators can set policies that determine which sites managed systems can access, create customized block messages, and prevent users from disabling the client software on managed systems.

NOTE: By default SiteAdvisor will block access to Red sites, display a warning message for Yellow sites but allow access, and allow access to Green and unrated (Gray) sites. By default Web Filtering for Endpoint does not block any sites based on their content categorization. We’ll see how to create a sample URL filtering policy below.

Ratings Enforcement on File Downloads

The following SiteAdvisor policy enables file download rating and email annotations. In other words, SiteAdvisor will enforce the Red\Yellow\Green rating on file downloads, as well as on the web sites themselves. For instance a site may have both Red and Green downloads. This policy would block the download of Red (dangerous) files, but allow the download of Green (safe) files.

1 Click the **System Tree** button on the favorites bar.
2 Highlight **My Organization**.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **SiteAdvisor Enterprise Plus 3.5**.
• On the line that lists **General**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **EASI General Policy**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.

Create custom policies

So far, we have assigned best practices policies that were created for you. At some point, you will have to create policies to accommodate some requirements on your network. In this section, we will create and assign two policies from scratch. This will show you the process from start to finish, and provide a better understanding of policy creation and management in ePolicy Orchestrator.

Locking the Local VirusScan Console

Follow these steps to create a new policy that prevents end users from tampering with the local VirusScan interface on their systems. VirusScan Enterprise runs on both workstations and servers; therefore, the VirusScan policies have separate settings for each platform. In this case, you want to make changes only to the workstation settings.

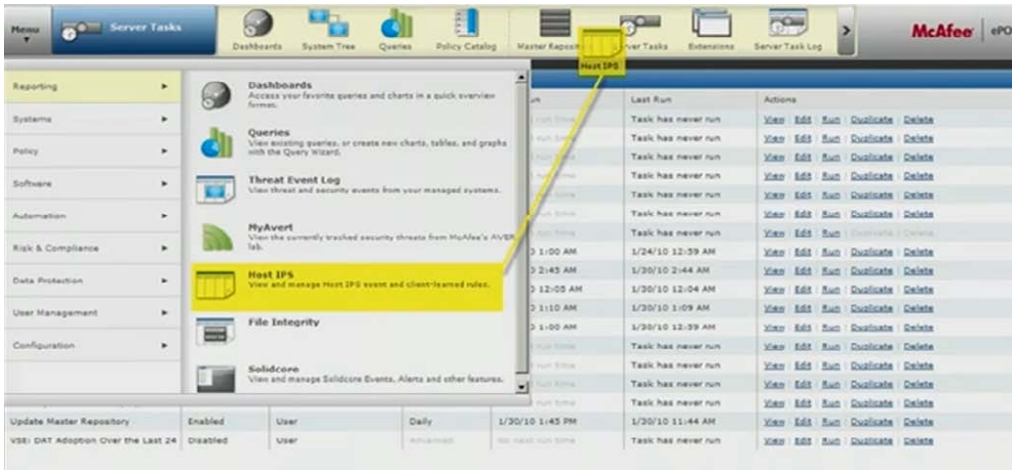
1 Click **Menu** | **Policy** | **Policy Catalog**.
2 From the **Product** drop-down menu, select **VirusScan Enterprise 8.8.0**.
3 From the **Category** drop-down menu, select **General Options Policies**.
4 On the line that lists **McAfee Default**, click **Duplicate**.
5 For **Name**, type Lock VSE Console, then click **OK**.
Note: It is wise to name policies in a way that describes their function. Use of "named policies" then makes it easier to assign them based on the role or function of systems.
6 Click **Lock VSE Console**, which now appears in the list of policies.
7 On the menu bar, click **Password Options**.
8 Make sure the **Settings for** option in the upper left is set to **Workstation**.
9 For **User interface password**, select **Password protection for all items listed**.
10 Type a password in the two boxes provided, then click **Save**.

As you might have noticed, the new policy was created by duplicating a default policy. Every policy you have assigned up to this point also began as a duplicate of the McAfee Default policy from the Policy Catalog. This new policy can now be assigned in the same manner as the policies above.

1 Click the **System Tree** button on the favorites bar.
2 Highlight **My Organization**.
3 Click the **Assigned Policies** tab.
• From the **Product** drop-down menu, select **VirusScan Enterprise 8.8.0**.
• On the line that lists **General Options Policies**, click **Edit Assignment**.
• For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
• From the **Assigned Policy** drop-down menu, select **Lock VSE Console**.
• Click **Save**. The policy is now assigned to that group and all its subgroups.

As noted, the above policy was designed specifically for systems with a workstation operating system. The local VirusScan console on servers will be accessible without a password.

Note: You can drag and drop commonly used items from the **Menu** onto the Favorites Bar at the top of the ePolicy Orchestrator interface, as shown in the figure below.



Variation on a Theme for Policy Creation and Application

In the previous example, you created the new policy in the **Policy Catalog**, then assigned it within the **System Tree**. In this example you will create and assign the new policy from the **System Tree**, achieving the same end result through an alternate workflow.

Blocking inappropriate websites with SiteAdvisor

The steps below guide you through the creation and assignment of a policy that blocks access to sites dealing with pornography or nudity and is applied to all systems.

1 Click the **System Tree** button on the favorites bar.
2 Highlight **My Organization**.
3 Click the **Assigned Policies** tab.
4 From the **Product** drop-down menu, select **SiteAdvisor Enterprise Plus 3.5**.
5 To the right of **Content Actions**, click **Edit Assignment**.
6 For **Inherit from**, select **Break inheritance and assign the policy and settings below**.
7 For **Assigned policy**, click **New Policy**.
8 Click the drop-down menu for **Create a policy based on this existing policy** and select **McAfee Default**.
9 For **Policy Name**, type My Blocked Categories, and then click **OK**. This opens the policy editor.
10 If prompted, click **OK** on the dialog box that says **Unsaved changes to this policy Assignment will be lost. Are you sure you wish to continue?**
11 Click the **Functional Group** drop-down menu and select **Pornography / Nudity**.
12 Click the check box beside **Content Category** to select all, then click the **Reputation** drop-down and choose **All** from the list.
13 Click **Block**, then click **Save**.
14 For **Assigned policy**, click the drop down and select **My Blocked Categories**, then click **Save** again on the **Policy Assignment** page.
15 Looking at the **Assigned Policies** column again, you will notice this policy has been assigned to the **My Organization** group and all its subgroups.

Remember you can break inheritance further down in the System Tree, as required, and assign a different policy at the subgroup level.

At some point you should take a little time to further explore the Policy Catalog. In addition to the McAfee Default policies, there are other pre-configured eASI policies that you can use. You can perform

tests by duplicating any policy and then make changes to the copy, thus keeping the original policy intact.

Set tasks for endpoints

So far you have created a System Tree, added some client systems, and created and assigned several policies. Next, you will schedule the deployment of VirusScan Enterprise and other security products. Product deployment is accomplished using a client task that the McAfee Agent retrieves and executes. Client tasks are also used for scheduled scans and updating.

The tasks themselves reside in the Client Task Catalog. Client tasks are independent, reusable objects. As such you can manage client task objects separately from their assignments and schedules. For example, you can assign a single client task to multiple locations, each with a unique schedule. Similar to the way ePolicy Orchestrator manages policies, you can create tasks in the Client Task Catalog and assign them in the System Tree. Alternatively you can create and assign client tasks directly from the System Tree.

Before Client Installation

Check if any other third party anti-virus product exists on your client systems. McAfee VirusScan Enterprise will check for the existence of 200+ anti-virus products, including previous versions of McAfee products. When VirusScan recognizes one of these programs, it will invoke the uninstaller for that software. To successfully deploy VirusScan and remove any third-party anti-virus software, ensure that you:

- Remove any client "uninstall password" option that is set in the third-party anti-virus software management console.
- Disable any client self-protection features set in the third-party anti-virus software management console.

While McAfee updates the anti-virus products list regularly, some products might not be recognized and removed automatically. In such cases, you should use native tools or scripts from your current vendor that will help you automate the removal.

Assigning the Deployment Tasks

In this section, you will assign the **EASI - Deploy Protection Suite - Endpoint** task to both the Workstations and Laptops groups. The task **EASI - Deploy Protection Suite – Server** will be assigned to the Servers group.

Note: A Deployment Task can be used to install one or more products. Deployment tasks are also used to upgrade existing products to newer versions, as well as uninstall McAfee products.

Assigning the Endpoint Deployment Task

The installer provided a pre-built Deployment Task for your Workstations and Laptops groups. The deployment includes ViursScan, Host IPS, SiteAdvisor, and Device Control. Follow these steps to assign the task to your groups.

1 Click the **System Tree** button**,** select the **Workstations** group, and then click **Assigned Client Tasks**.
2 Click **Actions**, then click **New Client Task Assignment**.
3 Under **Product**, select **McAfee Agent**.
4 Under **Task Type**, select **Product Deployment**.
5 Under **Task Name**, select the **EASI - Deploy Protection Suite - Endpoint**, and then click **Next**.

6 On the **Schedule** page, set the following options:
- Schedule status **Enabled**
- Schedule type **Run Immediately**

7 Click **Next**.
8 On the **Summary** page, click **Save**.
9 Repeat the above process for the **Laptops** group as well.

Assigning the Server Deployment Task

The installer provided a pre-built Deployment Task for your Servers group. The deployment includes VirusScan and SiteAdvisor. Follow these steps to assign the task to your Servers group.

1 Click the **System Tree** button**,** select the **Servers** group, and then click **Assigned Client Tasks**.
2 Click **Actions**, then click **New Client Task Assignment**.
3 Under **Product**, select **McAfee Agent**.
4 Under **Task Type**, select **Product Deployment**.
5 Under **Task Name**, select the **EASI - Deploy Protection Suite - Server**, and then click **Next**.
6 On the **Schedule** page, set the following options:
- Schedule status **Enabled**
- Schedule type **Run Immediately**

7 Click **Next**.
8 On the **Summary** page, click **Save**.

Note: When deploying to a large number of systems in a production environment, McAfee recommends scheduling a time window by using the **Randomization** option on the **Schedule** page. Task randomization allows you to deploy to a large number of nodes by staggering the time over which the task runs, thus preventing a flurry of simultaneous network requests. In a production environment, you might want to schedule deployments at specific times of the day. Setting the schedule here to **Run Immediately** simply speeds up the deployment process for evaluation purposes.

Assigning a Scheduled Scan Task

In this section, you will configure VirusScan to run a weekly scan for the Workstations group. There are two ways to do this. One can create tasks in the Task Catalog and assign them in the System Tree, as with the previous examples. (We assigned the pre-built Deployment and Update tasks above.) Alternatively, the workflow below allows for both the creation and assignment of the client task directly from the System Tree.

1 Click the **System Tree** button**,** select the **Workstations** group, and then click **Assigned Client Tasks**.
2 Click **Actions**, then click **New Client Task Assignment**.
3 Under **Product,** select **VirusScan Enterprise 8.0.0**.
4 Under **Task Type,** select **On Demand Scan**.
5 Under **Task Name,** select the **EASI – Full System Scan**, and then click **Next**.
6 On the **Schedule** page, set the following options:
- Schedule status **Enabled**
- Schedule type **Weekly**, and select the day(s) the scan should run.
- Start time is **12:00 AM**
- Select **Run once at that time**
- Select **Run Missed Task** with a delay of **10** minutes

7 Click **Next**.
8 On the **Summary** page, click **Save**.

You might subsequently create a similar task for the Laptops group, but provide additional flexibility, such as deferring scans while on battery power. One would typically establish separate schedules and exclusion configurations for scheduled scans of your various servers based on services they support (e.g., Exchange, SharePoint, SQL, Domain Controller, DHCP, etc.).

Create client tasks

Creating an Update Task

While a pre-built Product Update task was provided, it is important to walk through the process once in order to see the whole process.

In this section, you will create a client task that updates the VirusScan DATs and the Host Intrusion Prevention content. In a production deployment you may prefer separate schedules for groups containing servers and workstations. The schedule below is only a sample. Feel free to set a different schedule if desired.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **My Organization** group.
Click the **Assigned Client Tasks** tab.
3 Click **Actions**, and then click **New Client Task Assignment**.
4 Under **Product**, select **McAfee Agent**. Under **Task Type**, select **Product Update**, and then click **Create New Task**.
5 For **Name**, type AV & HIPS Daily Update.
6 Next to **Package Types**, make sure the following boxes are checked:

- **Engine**
- **Buffer Overflow DAT for VirusScan**
- **Host Intrusion Prevention Content**
- **DAT**

7 Click **Save.**
8 When returned to the Client Task Assignment Builder page, highlight **AV & HIPS Daily Update** on the right under **Task Name**, and then click **Next**.
9 On the **Schedule** page, set the following options:

- Set Schedule Type to **Daily**
- Set Start Time to
- Set Start Time to **4:00 pm** and any Repeat if desired.
- Select **Run Missed Task** with a **5 minute** delay.

10 Click **Next**.
11 On the **Summary** page, click **Save**.

A Note Regarding Laptops

Laptops that temporarily disconnect from your network continue to run their assigned update tasks. By default, laptops retrieve updates from the McAfee site while on the road with an available Internet connection. If you have a large number of laptops that you'd like to have visibility of, and manage them when they are on the road, whether a VPN is present or not, consider placing an ePolicy Orchestrator "Agent Handler" in your DMZ. Additional information on Agent Handler is located in the ePolicy Orchestrator product guide and in the ePolicy Orchestrator Agent Handler White Paper.

Policy and task inheritance in the System Tree

Policies

By now you have noticed a recurring phrase when assigning policies and tasks. Namely "*The policy (or task) is now assigned to that group and all its subgroups*." In short, child objects (subgroups and individual systems) inherit settings from their parent container unless you break inheritance at a specific point in the tree. Recall the File Reputation policies for VirusScan that you applied earlier. We broke inheritance on the Laptops group, and assigned the *High* protection level instead, since those systems are often more exposed than those on the internal network.

Note: If you assign policies for a product to a group of systems where that product is not installed, there is a zero sum effect. Since that particular product is not installed, the policy has no effect on those systems.

Client Tasks

The inheritance concept is similar to that of Client Tasks when breaking inheritance at the subgroup or individual system level. At that point, your choices range from selecting a different task from the Client Task Catalog, to making a simple scheduling change without affecting the rest of the task's settings.

Viewing Broken Inheritance

ePolicy Orchestrator provides easy visibility of broken inheritance within the System Tree.

1 Click the **System Tree** button on the favorites bar.
2 Highlight **My Organization**.
3 Click the **Assigned Policies** tab.
4 From the **Product** drop-down menu, select **VirusScan Enterprise 8.8.0**.
5 On the line that lists **On-Access General Policies**, note the **Broken Inheritance** column states **1 doesn't inherit**. The ability to drill down on broken inheritances provides a way to both view and reset any policies that may have been applied in incorrectly.
6 Click on the **1 doesn't inherit** link to see the list of objects that do not inherit that policy from the My Organization container. In this case, it is just the Laptops group. Note that the **Actions** button provides an option to reset inheritance if that is ever required.
7 Click **Close**.

Deploy the McAfee Agent

The McAfee Agent is the distributed component of ePolicy Orchestrator. It must be installed on each system in your network that you wish to manage. The agent collects and sends event information at intervals to the ePolicy Orchestrator server. It also installs and updates the endpoint products, and applies your endpoint policies. Systems cannot be managed by ePolicy Orchestrator unless the McAfee Agent is installed.

The steps taken so far have focused on populating the System Tree, as well as creating and assigning policies and tasks. With those now in place you can begin to deploy protection on your systems. Again, based on their location in the tree, managed systems will inherit the policies and tasks of their parent container. With the Deployment tasks assigned, you will now push the McAfee Agent. By installing the Agent, the clients will begin communicating with ePolicy Orchestrator, download and install protection based on configured tasks, and enforce policies specific to the products installed.

Before deploying the McAfee Agent, you should verify both communication between the server and systems, and access to the default Admin$ share directory on the client. If your test systems are not part of a domain, you can simply copy **Framepkg.exe** to your client systems and execute it locally when we reach that step. **Framepkg.exe** is located on the ePolicy Orchestrator server in one of the following directories:
C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409
or
C:\Program Files(x86)\McAfee\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409

1 Check that you can ping client systems by name. This demonstrates that the server can resolve client names to an IP address.
2 Assuming Active Directory Domain, check for remote access to the default Admin$ share on the client systems:

- From the ePolicy Orchestrator server click **Start | Run**, then type \\computer-name\admin$, where *computer-name* is the NetBIOS name of one of the client systems. If the systems are properly connected over the network, your credentials have sufficient rights, and the Admin$ shared folder is present, a Windows Explorer dialog box opens.

3 If an active firewall is running on any client systems, you may need to create an exception for **Framepkg.exe**. This is the McAfee Agent that ePolicy Orchestrator pushes to the systems you will manage. Alternatively, you can disable the client firewall.

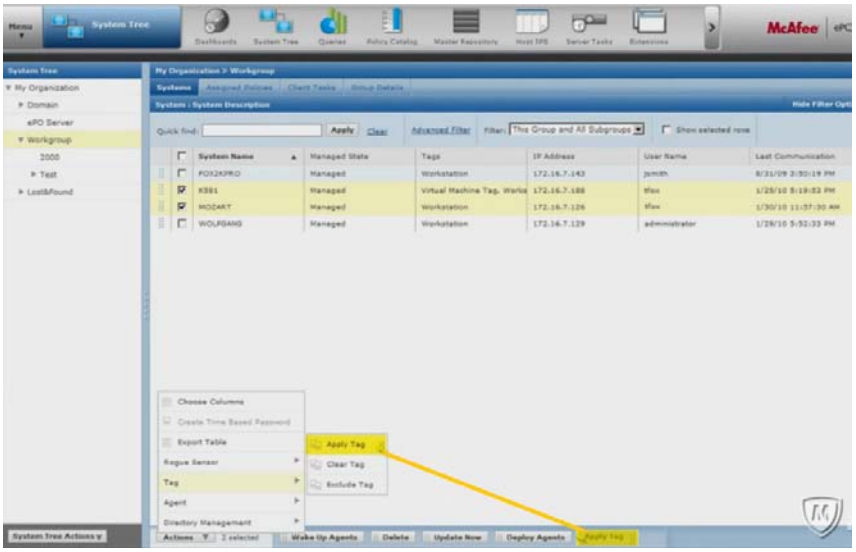
Deploying the McAfee Agent

As previously mentioned, a Windows domain is not a requirement to use ePolicy Orchestrator, but there are certain advantages when used in the context of a domain. One of those is the installation of the management agent known as the McAfee Agent. ePolicy Orchestrator pushes this installer to Admin$ share on your test systems and installs with Domain Admin credentials you specify. In fact this is the only installation that uses a push method. Once the Agent is installed, clients will pull the various endpoint protection components for installation.

It is assumed you have a limited number of test systems (under 50), so we will push the Agent to all the machines in the System Tree.
1 Click the **System Tree** button on the favorites bar.
2 Highlight the **My Organization** group.
3 Click the **Systems** tab.
4 Change the **Preset** drop-down to **This Group and All Subgroups** to view all the systems.
5 Check the box next to the column heading **System Name**. This selects all the systems.
6 Click **Actions** | **Agent** | **Deploy Agents**.
7 For **Credentials for agent installation:** type credentials that have rights to install software on client systems, such as a Domain Administrator account (domain\administrator), and click **OK**. If desired, you can select the option **Remember my credentials for future deployments**.
8 The **Server Task Log** appears showing the status of the Agent push.

It will take a few minutes for the McAfee Agent to install and for client systems to retrieve and execute the installation packages for the endpoint products. When first installed, the Agent determines a random time up to 10 minutes before its initial communication to the ePolicy Orchestrator server to retrieve policies and tasks.

Note: You can drag and drop commonly used items from the **Actions** button onto the taskbar at the bottom of the ePolicy Orchestrator interface, as shown in the following figure.



Verifying agent communication with ePolicy Orchestrator

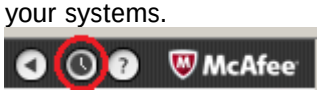
Once the initial agent-server communication has occurred, the agent polls the server once every 60 minutes by default. This is known as the Agent to Server Communication Interval or ASCI. Earlier we applied a policy that changed that interval to 120 minutes. Every time this occurs, the Agent polls ePolicy Orchestrator to upload client events and retrieve any applicable policy or task changes.

With an ASCI of 120 minutes, an agent that polled the server 30 minutes ago will not pick up any new policies for another 90 minutes. However, you can always force systems to poll the server with an Agent Wake Up Call. The Wake Up Call is useful when you need to force a policy change sooner than the next communication would occur. It can also be used to force clients to run tasks on demand, such as an immediate update or scan.

Sending an Agent Wake Up Call

Send a Wake Up Call to force polling by clients who have not yet communicated with the ePolicy Orchestrator server.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **My Organization** group.
3 Click the **Systems** tab.
4 Change the **Preset** drop-down to **This Group and All Subgroups** to view all the systems.
5 If the IP addresses and user names are listed, the agent on the client system is communicating with the server.
6 If five to ten minutes pass and systems do not display an IP address and user name, select all systems, click **Actions** | **Agent** | **Wake Up Agents,** and click **OK**.
7 You may need to click the **Refresh** button in the ePolicy Orchestrator console to view status change for your systems.



ePolicy Orchestrator Refresh button

Note: If sending a Wake Up Call fails to populate the client's IP address and user name, other environmental factors might be preventing the initial agent deployment. If this happens, simply copy the agent installer, **Framepkg.exe**, located on the ePolicy Orchestrator server, and run it locally on your test systems. Verify that a host or network firewall is not blocking agent communication to the server.

There are many additional ways to deploy the McAfee Agent, such as login scripts or third-party deployment tools. See the ePolicy Orchestrator Product Guide or online help.

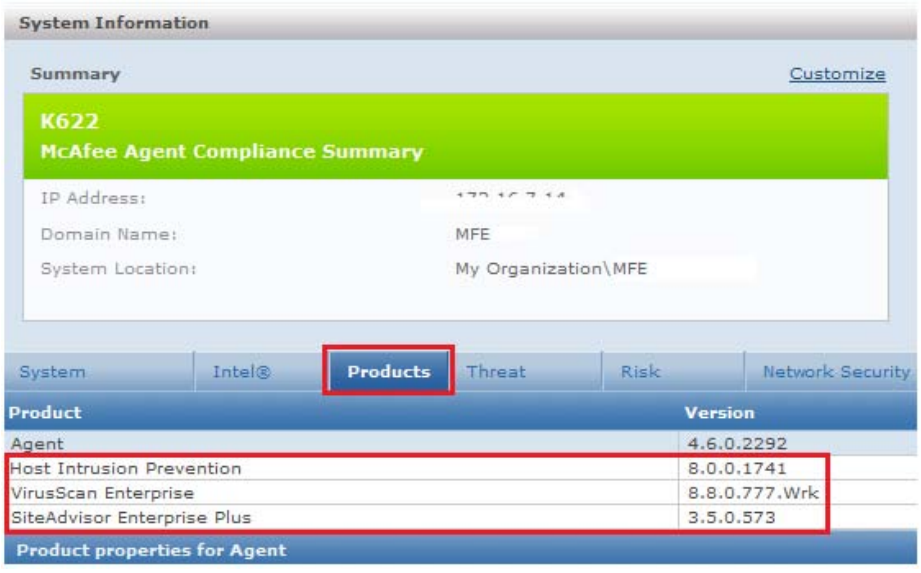
Quick Tip: The following video provides a short overview of the Wake Up Call: Purpose of the Agent Wakeup Call.

Verifying Endpoint Protection Installation

Depending on how many products you deployed, the client installation process will take several minutes to complete. At that point you can verify client installations from the ePolicy Orchestrator server or on the client systems themselves by right-clicking the McAfee system tray icon.

Follow these steps to verify client installations from the ePolicy Orchestrator server. You should allow several minutes for the client installations to complete.

1 Click the **System Tree** button on the favorites bar.
2 Highlight the **My Organization** group.
3 Click the **Systems** tab.
4 Change the **Preset** drop-down to **This Group and All Subgroups** to view all the systems.
5 Click on one of your systems to view its **System Information** page.
6 Click the **Products** tab on the System Information page to view information about McAfee components installed on this node, similar to the example below.



Revisiting the Deployment Task Assignment at Some Point

The intent of the pre-built Deployment Tasks is to install the endpoint protection modules on a few test clients and servers. We configured the Deployment tasks to *Run Immediately*, since bandwidth impact is minimal for deployment to a small number of test systems. If you decide to use this installation of

ePolicy Orchestrator in a production environment, you should revisit the setting of those task assignments at some point. Whether you choose a specific time of day for installations or leave the schedule as *Run Immediately*, you should add a window of Randomization to stagger the installations over a period of several minutes or hours, to avoid a flurry of simultaneous requests across the network. The randomization window chosen is dependent on several factors, but primarily the number of systems to which you are deploying and whether the installations are at local or remote sites.

Quick Tip: As opposed to performing a large number of remote installations to systems in different sites, ePolicy Orchestrator allows you replicate the files necessary for installations and updates to "distributed repositories" at strategic locations across your network. See the Quick Tip video Why and How to Create Distributed Repositories. One preferred type of distributed Repository is the Super Agent. Also see the Quick Tip video The Use of Super Agents. If applicable, an Agent Handler may be used.

Use dashboards and queries

Dashboards and queries provide various types of status information about your environment. Each product in the Endpoint Protection suites has predefined queries that you can run individually. Often the queries cover recent events, such as detections in the last 24 hours or 7 days, or they might provide trending information over time. ePolicy Orchestrator also includes several predefined dashboards. Dashboards are comprised of multiple queries or other objects. You can also create custom dashboards and queries. By default, there are several active dashboards available for viewing. You can also create custom dashboards by using default queries or ones that you create. In the sections below, we will examine some of the default dashboards and queries, create a custom query, and create a custom dashboard.

Dashboard Overview

While there may not yet be much event data to report, this is a good opportunity to examine some of the default dashboards and understand how they are created.

1 Click the **Dashboards** button on the favorites bar.
2 From the **Dashboard** drop-down, choose **VSE: Current Detections**.
This dashboard breaks down various types of detections made by VirusScan Enterprise, specifically viruses, spyware, and other unwanted programs for the last 24 hours and last 7 days. You likely don't have any detections showing yet, but now you know where to find that data. (You can use the well known anti-virus test string **EICAR.COM** file from http://www.eicar.org for testing and generating immediate detections.)
3 From the **Dashboard** drop-down, choose **Host IPS: Signatures Triggered**.
Elements of this dashboard will be helpful when tuning Host IPS. It provides a breakdown of triggered signatures by severity for both workstations and servers.
4 From the **Dashboard** drop-down, under **Public Dashboards**, choose **ePO Summary**.

Query Overview

In this section we will run a predefined query and view the results.

1 Click the **Queries & Reports** button on the favorites bar.
2 Expand the **Shared Groups** on the left. Each group contains a number of predefined queries.
3 Highlight the **VirusScan Enterprise** group.
4 Scroll down the alphabetical list of queries, locate **VSE: DAT Deployment**, and click **Run** at the far right. Assuming VirusScan has been installed and has performed its initial DAT (signature) update, you

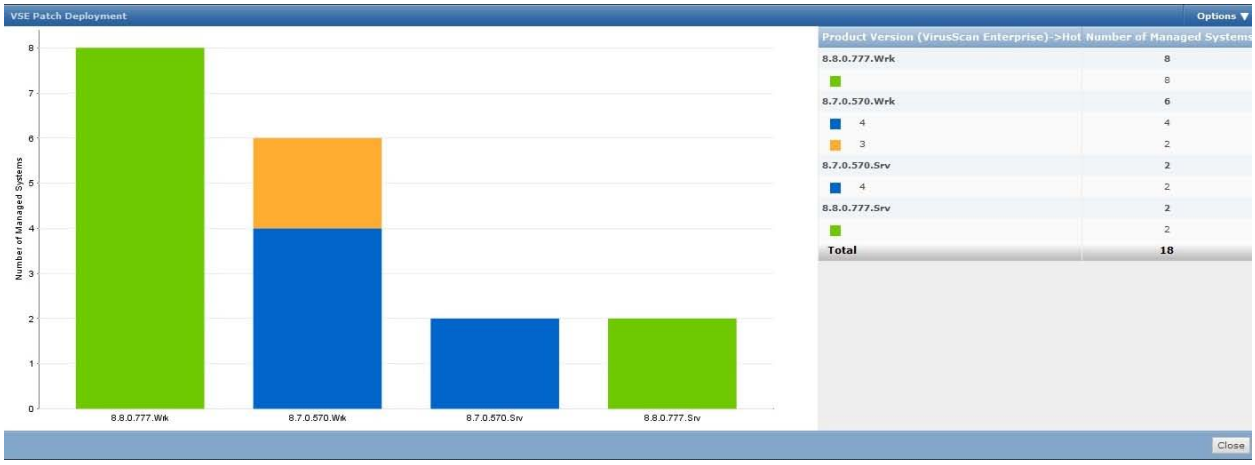
will see a pie chart. If all test systems are running the same DAT, the pie chart will display only one color. However, this is an important query to watch going forward, so you will know at a glance if all your clients are current on their virus signatures.
5 Click **Close**. We will revisit this query again.

Creating a Custom Query

ePolicy Orchestrator also provides a wizard that allows you to create custom queries, which can also be used in a dashboard. In this section, you will create a more advanced query that displays both the version and patch level of VirusScan installations, broken down by servers and workstations.

1 Click the **Queries & Reports** button on the favorites bar.
2 At the bottom of the page, click **New**.
3 Make sure **System Management** is highlighted on the left, select **Managed Systems** under Result Types, and then click **Next**.
4 Select **Stacked Bar Chart** on the left, under Display Results As.
5 For **Stack Labels Are**, scroll down and select **Product Version (VirusScan Enterprise)** under VirusScan Enterprise Properties.
6 For Bar Labels Are, scroll down and select **Hotfix/Patch Version (VirusScan Enterprise)** under VirusScan Enterprise Properties, and then click **Next**.
7 Under Available Columns on the left, click the arrow next to **IP Address** under Computer Properties to add it to the column list on the right, and then click **Next**.
8 On the Filter page, click **Run**. Your results will appear homogeneous, as all your test machines are running the same version and patch level of VirusScan. As future product patches are released, it is helpful to be able to report on any unpatched systems. This report will provide that visibility at a glance, as well as display any systems where VirusScan is not installed.
9 Click **Save**.
10 On the Save Query page, provide a name for the query, such as VSE: Version w\Patch Level.
11 Select **VirusScan Enterprise** from the Existing Group drop-down, then click **Save**. Your new query is now listed alphabetically in the VirusScan query group. You can run this query at any time or use it in a dashboard.

Here's the output of this sample query, showing several systems running different versions of VirusScan. The green bars show workstations and servers running VirusScan 8.8 with no patch. The blue areas indicate workstations and servers with VirusScan 8.7 with Patch 4, while the yellow section shows three workstations running VirusScan 8.7 with only Patch 3.



Drilling down on the yellow section provides details regarding those specific systems still running VSE 8.7 with Patch 3. Of course, product patches and new product versions can be deployed using ePolicy Orchestrator and would be updated in under normal circumstances. This sample query is provided to

give you an idea of the level of detail available for reporting. Note that it is not necessary to upgrade the version of ePolicy Orchestrator in order to upgrade client versions.

Creating a Custom Dashboard

In this section you will create a new dashboard utilizing the query just created along with some other useful default queries.

1 Click the **Dashboards** button on the favorites bar.
2 Click the **Dashboard Actions** drop-down and choose **New**.
3 Provide a name for the dashboard, such as Endpoint Status, select **Public** for *Dashboard Visibility*, and then click **OK**.
4 You are then presented with a blank dashboard. Click the **Add Monitor** button.
5 Use the arrows to scroll through the Monitor Gallery toolbar and locate **Queries**. Drag the **Queries** object down on to the blank dashboard.
6 In the New Monitor box that appears, select your new query **VSE: Version w\Patch Level** under Shared Groups-VirusScan Enterprise, and then click **OK**.
7 Repeat this process by again dragging the **Queries** object to a gray area either below or to the side of the first monitor. Note that the box is shaded as you drag it. It will state "Monitor will not fit here" if you attempt to place it on top of another monitor. Choose the query titled **VSE: DAT Deployment**. Note the monitors will resize themselves automatically. Repeat this process adding two additional queries: **Host IPS: Desktop High Triggered Signatures** and **Host IPS: Desktop Medium Triggered Signatures**. You can add additional monitors as desired, but note the more monitors you add, the smaller they will appear on the dashboard. Optionally, you may choose to create distinct dashboards per product showing the installation count, update status, and recent detections for VirusScan, and a separate dashboard for Host IPS.
8 Click **Save** in the upper right corner, and then click **Close** in the upper left to return to the main Dashboards page.
9 From the **Dashboard** drop-down, you can now choose your *VirusScan Status* dashboard, listed under Private Dashboards. It is only visible under your login. By clicking the **Dashboard Actions** drop-down and choosing **Edit**, you can make your dashboard Public and, therefore, usable by other users of ePolicy Orchestrator.

Quick Tip: These videos provide additional examples and use cases around ePolicy Orchestrator queries and as well as customizing and scheduling reports:
Quick Tips: Dashboard Reports
Quick Tips: Advanced Reporting

Summary

Congratulations! By completing this guide, you have completed many of the common tasks used in creating and maintaining a secure endpoint environment with ePolicy Orchestrator.

What you accomplished

1 Installed the core components of the McAfee Endpoint Protection suites
2 Enabled and ran a task that updates the ePolicy Orchestrator master repository from the McAfee site
3 Leveraged the pre-built System Tree structure and added test systems into groups
4 Applied a new policy that enables remote access to the Agent Log on client systems
5 Created and\or applied new endpoint policies for the following:

- VirusScan Enterprise
- SiteAdvisor Enterprise
- Web Filtering for Endpoint
- Host Intrusion Prevention – IPS (EPA Suite only) and Host Firewall

6 Assigned a deployment task to install VirusScan, Host Intrusion Prevention, and SiteAdvisor Enterprise on your test systems
7 Created an update task to keep your systems current
8 Created a VirusScan On Demand scan task
9 Deployed the McAfee Agent, verified agent-server communication, and verified client installs
10 Viewed some of the available default dashboards, and ran a predefined query
11 Ran a default query and created custom one
12 Created a custom dashboard from default and custom queries

What we didn't have time to cover

- Scheduling reports
- Role based access
- More on queries and reports
- Tags and tag based management
- Setting up alerts with Automatic Responses
- Utilizing Software Manager to download additional licensed or evaluation software
- Distributed Repositories to provide installation and updating points for remote locations
- Using an Agent Handler for ePolicy Orchestrator load balancing or to manage mobile users when no VPN is present
- Management of other McAfee offerings for Windows, Macintosh, and Linux
- Management of McAfee-compatible products from Security Innovation Alliance partners

There's a lot more to see...

Appendix A: McAfee Device Control

Note: In an Active Directory domain, you can leverage user based policies with Device Control. In Workgroup mode, only local user or machine-based policies are possible.

Post-Installation Configuration

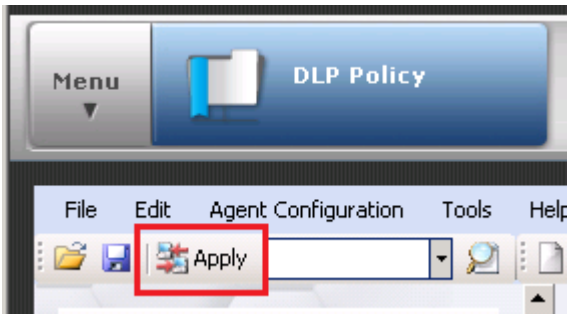
The installer automatically checks McAfee Device Control into the ePolicy Orchestrator software repository; however, additional steps need to be taken to properly configure Device Control for use. The following steps take you through the installation of the McAfee DLP Management Tools, as well as checking in a starter policy that makes all USB storage devices function as read-only unless they are McAfee Encrypted USB drives.

Initializing the DLP Interface

1 In the ePolicy Orchestrator console, select **Menu | Data Protection | DLP Policy**.
2 The McAfee DLP Endpoint Management Tools installer runs, and, after a brief delay, the DLP Management Tools Setup wizard appears. Depending on your browser settings, you may be prompted to install the ActiveX control.
3 Click **Install**, then click **Next** on all defaults provided in the wizard, and then click **Finish**.
4 Click **OK** on the dialog box that states "DLP Global Policy is Unavailable".
5 When a first-time initialization page appears, click **Cancel**. (If you clicked **Next**, just click **Cancel** at your earliest opportunity.)

Importing policies

1 From the DLP Policy interface, we will import a starter policy by navigating to **File | Open**.
2 Click **Yes** on the dialog box that states "This operation will discard the current policy".
3 Browse to the **Post Install** directory where you extracted the installer download.
4 Select **EASI - Global Policy.OPG**, and then click **Open** to import the policy.
5 Click **Apply** on the toolbar in the DLP Policy interface, as shown below.



Evidence and Whitelist Folders

Two folders must be created and shared, and their properties and security settings must be configured appropriately. The folders do not need to be on the same computer as ePolicy Orchestrator, but it is usually convenient to put them there.

Create the following directory structure on the ePolicy Orchestrator server:

- c:\dlp_resources\
- c:\dlp_resources\evidence
- c:\dlp_resources\whitelist

Configure the Share Names and Permissions

Configuration of the folders on Windows 2008 Server for Device Control requires specific security settings.

Configuring the Evidence folder

1 Right-click the evidence folder and select **Properties**.
2 Select the **Sharing** tab, then click **Advanced Sharing**. Select the **Share this folder**.
3 Modify the Share name to evidence$.
NOTE: The $ ensures that the share is hidden.
4 Click **Permissions**. With the default user name Everyone selected, allow **Full Control**, and then click **OK**.
5 Select the Security tab, and then click **Advanced**.
6 On the Permissions tab, click **Change Permissions**, and then deselect the **Include inheritable permissions from the object's parent** option.
7 A confirmation message explains the effect this change will have on the folder. Click **Remove**. The Permissions tab on the Advanced Security Settings dialog box now shows all permissions eliminated.
8 Click **Add** to select an object type.
9 In the **Enter the object name to select** text box, type Domain Computers, then click **OK**.
The **Permission Entry** dialog box is displayed.
10 In the **Allow** column, select **Create Files/Write Data** and **Create Folders/Append Data**. Verify that the **Apply to** option says **This folder, subfolders and files**, then click **OK**.
The Advanced Security Settings dialog box now includes Domain Computers.
11 Click **Add** again to select an object type.
12 In the **Enter the object name to select** text box, type Domain Admins (or another security group if desired), then click **OK** to display the Permission Entry dialog box.
13 In the **Allow** column, select **Create Files/Write Data** and **Create Folders/Append Data**. Verify that the **Apply to** option says **This folder, subfolders and files**, then click **OK**.
The Advanced Security Settings dialog box now includes Domain Admins.
14 Click **OK**, **OK**, and then **Close** on the remaining dialog boxes.

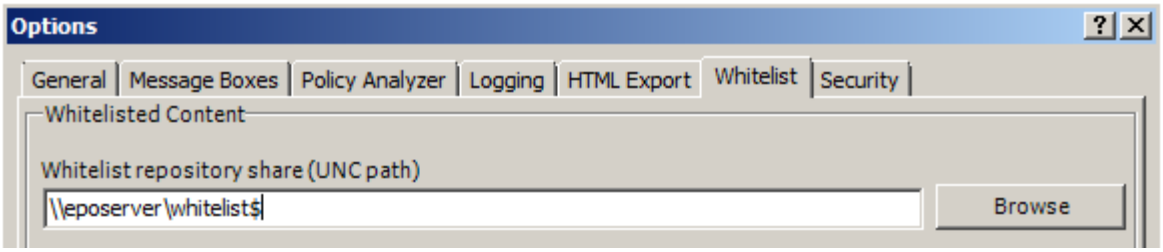
Configuring the Whitelist folder

1 Right-click the whitelist folder and select **Properties**.
2 Select the **Sharing** tab, then click **Advanced Sharing**. Select the **Share this folder**.
3 Modify the Share name to whitelist$, and click **OK**.
NOTE: The $ ensures that the share is hidden.
4 Click **Permissions**. With the default user name Everyone selected, allow **Full Control**, and then click **OK**.
5 Select the Security tab, and then click **Advanced**.
6 On the Permissions tab, click **Change Permissions**, and then deselect the **Include inheritable permissions from the object's parent** option.
7 A confirmation message explains the effect this change will have on the folder. Click **Remove**. The Permissions tab on the Advanced Security Settings dialog box now shows all permissions eliminated.
8 Click **Add** to select an object type.
9 In the **Enter the object name to select** text box, type Domain Computers, then click **OK**.
The **Permission Entry** dialog box is displayed.
10 In the **Allow** column, select **List Folder/Read Data**. Verify that the **Apply to** option says **This folder, subfolders and files**, then click **OK**.
The Advanced Security Settings dialog box now includes Domain Computers.
11 Click **Add** again to select an object type.
12 In the **Enter the object name to select** text box, type Domain Admins (or another security group if desired), then click **OK** to display the Permission Entry dialog box.

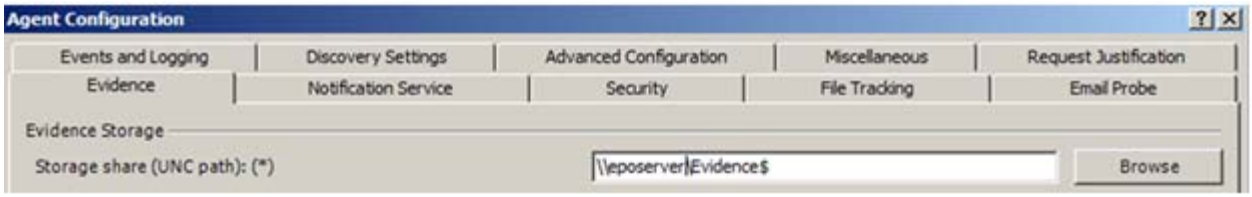
13 In the **Allow** column, select **Create Files/Write Data** and **Create Folders/Append Data**. Verify that the **Apply to** option says **This folder, subfolders and files**, then click **OK**.
The Advanced Security Settings dialog box now includes Domain Admins.
14 Click **OK**, **OK**, and then **Close** on the remaining dialog boxes.

Finalizing Configuration

1 In the ePolicy Orchestrator console, select **Menu | Data Protection | DLP Policy.**
2 Select **Tools | Options** and select the **Whitelist** tab. Update the field with the applicable whitelist share that was created. Click **OK**.



3 Select **Agent Configuration | Edit Global Agent Configuration** and select the **Evidence** tab. Update the field with the applicable evidence share that was created. Click **OK**.



4 Click the **Apply** on the DLP Policy interface to save all settings.

NOTE: The Deployment task for your Workstations and Laptops groups already included Device Control, but it was deployed without a policy. The next time those clients poll the server, they will see this new policy, download it, and begin enforcing it locally.

Appendix B: List of included eASI best practice policies

The installer has been bundled with many best practice policies for the McAfee Endpoint Protection suites. These starter policies include common best practice settings for VirusScan Enterprise, Desktop Firewall, McAfee Agent, and Device Control. As every environment is different, these policies should be thoroughly reviewed and modified to meet the needs of your specific environment. This section will highlight the best practice policies that have been bundled with the installer.

McAfee Agent 4.6

General

The following policy allows administrators to view the McAfee Agent log on a remote client. It also increases the Agent to Server Connection Interval from one hour to two:

- EASI - General

VirusScan Enterprise 8.8

Access Protection Policies

Policies supply exclusions specific to systems running McAfee Endpoint and McAfee Security for Microsoft Exchange (MSME). The endpoint policy can be applied to servers and workstations. The Exchange policy need only be applied to servers running both MSME and VirusScan Enterprise.

- EASI - McAfee Endpoint Protection Suite Clients
- EASI – Microsoft Exchange Servers

On-Access Default Processes Policies

The following policies have common file & directory exclusions and other optimizations specific to certain server types. These policies are assigned to a group or system in conjunction with the corresponding Low-Risk Processes Policies below that share the same name:

- EASI - Default: AD Domain Controller
- EASI - Default: DHCP and WINS Servers
- EASI - Default: Lotus Notes\Domino Servers
- EASI - Default: McAfee Endpoint Protection Clients
- EASI - Default: ePolicy Orchestrator Server
- EASI - Default: MS Exchange Servers
- EASI - Default: MS SharePoint Servers
- EASI - Default: MS SQL Servers

On-Access Low-Risk Processes Policies The following policies have common file & directory exclusions and other optimizations specific to certain server types. These policies are assigned to a group or system in conjunction with the corresponding Default Processes Policies above that share the same name:

- EASI - Low: AD Domain Controller
- EASI - Low: DHCP and WINS Servers
- EASI - Low: Lotus Notes\Domino Servers
- EASI - Low: McAfee Endpoint Protection Clients
- EASI - Low: ePolicy Orchestrator Server
- EASI - Low: MS Exchange Servers
- EASI - Low: MS SharePoint Servers
- EASI - Low: MS SQL Servers

KB66909 is the Master Exclusions KB article for VirusScan Enterprise.

On-Access General Policies
While the Default for GTI is Medium, the policy for High could be applied to those systems most likely to encounter malware, such as laptops:

- EASI - Enable GTI for On-Access (High)

Host Intrusion Prevention 8.0: General

Client UI (Windows)
The Initial Testing policy below allows the local user to disable any FW & IPS functions. It would typically be used during a testing phase. The Production policy removes end user control to prevent tampering in the future.

- EASI – Initial Testing (pre-deployment)

- EASI – Production

Host Intrusion Prevention 8.0: Firewall

Firewall Options (Windows)
The following policy enables the Firewall and activates GTI protection:

- EASI – Enable FW and GTI

Firewall Rules (Windows)
This policy allows for immediate implementation of McAfee GTI without the need to set any other specific firewall rules.

- EASI – GTI Only

Host Intrusion Prevention 8.0: IPS

IPS Options
When Host IPS is first installed the protection is not active. You must enable protection in the IPS Options policy and apply the policy to the client.

This policy enables Host IPS, as well as Network IPS which detects and prevents known network-based attacks arriving at the host system.

- EASI - HIPS and NIPS enabled

In addition to the policy above, this one adds Adaptive Mode functionality. To automate the creation of exception rules, clients are placed in Adaptive mode. In this mode, client rules are created without interaction from the user. After client exception rules are created, you need to carefully analyze them and decide which to convert to server-mandated policies.

- EASI - HIPS and NIPS enabled (adaptive mode)

A subset of the above, this policy is used to activate Host IPS protection only.

- EASI - HIPS enabled

IPS Protection
After all the required components for Host IPS are installed and communicating, you are ready to apply protection, monitor events, and update policies and content as needed.

Similar to the default Enhanced Protection, this policy blocks High and Medium events and also logs Low severity events. Only block Medium events after first logging and reviewing them to see if any exceptions should be created.

- EASI - Block High and Medium events

Only High severity events are blocked; Medium and Low events are only logged.

- EASI - Block High events

Also a good starter policy but only logs High, Medium and Low severity events without any blocking.

- EASI - Initial monitoring (pre-blocking)

IPS Rules
These policies define the signatures, exceptions, and application protection rules to be used.

As virtual systems are often used for evaluations, assigning this policy facilitates testing by changing VMWare-related signatures to a severity of Low.

- EASI - VMware exception policy

SiteAdvisor Enterprise 3.5

Authorize List (UBP)
The following policy ensures that sites specifically listed in the Authorize Policy are allowed even if listed in the Prohibit Policy:

- EASI – Authorize Policy

Enable/Disable (UBP)
Applied to a group or subgroup, the Disable policy below can quickly deactivate SiteAdvisor on the client systems. Assigning a different policy such as the McAfee Default or another policy to Enable will reactivate SiteAdvisor Enterprise on those systems.

- EASI – Disable SAE Policy

General (UBP)
The following policy enables file download and email annotations rating:

- EASI – General

DLP / Device Control 9.2

Device Rules

Accessible from the DLP Policy page in ePolicy Orchestrator, this policy makes USB storage function as read-only unless they are McAfee Encrypted USB drives. You can alter this policy to allow other USB drives but track usage:

- Read-Only USB Storage Except for McAfee Encrypted USB Drives

Appendix C: References

Use the links in this section to access additional information.

Support by seeing

ePO Deep Dive – provides an extensive overview of ePolicy Orchestrator's capabilities:
Deep Dive into McAfee ePolicy Orchestrator

Quick Tips videos for ePolicy Orchestrator can be found here:
ePO Quick Tips

Quick Tips videos for many other McAfee products can be found here:
McAfee Quick Tips

Video Tutorials from McAfee Technical Support
Video tutorials

Support by reading

McAfee Security Connected Reference Architecture

Security Connected Reference Architecture Homepage
Security Connected: Optimize Your Business
Security Connected for Financial Services

Global Threat Intelligence (GTI)

McAfee GTI Reputation & Categorization Services
GTI Webinar Recording & Materials
How to enable Global Threat Intelligence Technology in your McAfee product

Search the Knowledge Base
Search McAfee's award-winning Knowledge Base to find answers to questions.

Product Documentation

McAfee product documentation is located on the Customer Portal.

ePolicy Orchestrator 4.6

- ePolicy Orchestrator 4. 6 Product Guide
- ePolicy Orchestrator 4.6 Installation Guide
- ePolicy Orchestrator 4.6 Log files Reference Guide
- ePolicy Orchestrator 4.6 - Master list of release Support articles
- Release Notes for ePolicy Orchestrator 4.6

VirusScan Enterprise 8.8

- VirusScan Enterprise 8.8 Installation Guide
- VirusScan Enterprise 8.8 Product Guide
- VirusScan Enterprise 8.8 Best Practices Guide
- VirusScan Enterprise 8.8 Patch 1 Release Notes

McAfee Host Intrusion Prevention 8.0
- Host Intrusion Prevention 8.0 Installation Guide
- Host Intrusion Prevention 8.0 for Product Guide
- Host Intrusion Prevention 8.0 Release Notes
- Host Intrusion Prevention 8.0 ClientControl.exe Utility Readme
- Access Protection in McAfee VirusScan Enterprise and Host Intrusion Prevention – Whitepaper

SiteAdvisor Enterprise 3.5
- SiteAdvisor Enterprise 3.5 Installation Guide
- SiteAdvisor Enterprise 3.5 Product Guide
- SiteAdvisor Enterprise 3.5 Release Notes
- Resources for Site Owners and Consumers

Support by doing

Download Software Updates
Obtain the latest anti-virus definitions, product security updates and product versions. To get product patches and maintenance releases you must be logged on to the Service Portal.

Global Solutions Lab
Configure and test common scenarios in a virtual environment.

Security Advisories
Subscribe to McAfee Security Advisories.